1. UVOD

UICT sustavima postoji veliki broj izvora sigurnosnih informacija i statusa. Osigurati zaštitu informacijskog sustava je težak zadatak. Što je sustav veći, s većim brojem zaposlenika, teže je to učiniti. Organizacije se suočavaju s brojnim sigurnosnim prijetnjama poput računalnih prijevara, špijunaže, sabotaže, vandalizma, požara, poplave i sl. Šteta nanesena organizaciji u obliku zloćudnog koda, računalnog hakiranja i uskraćivanja usluge je sveprisutnija pojava.

Različiti uređaji generiraju velike količine logova koje je vrlo teško pratiti i analizirati u realnom vremenu pa se često događa da neke incidente primijetimo prekasno ili ih uopće ne primijetimo. Logovi (eng. logs) su generirani zapisi bilo kojeg uređaja ili softvera unutar ICT sustava. Logovi nam daju povratnu informaciju o statusu uređaja ili njegove aktivnosti u realnom vremenu.

Security Informationand Event Management[1] (SIEM) sustavi su rješenja za prikupljanje, normalizaciju i automatiziranu analizu sigurnosnih događaja i logova sa različitih uređaja u realnomvremenu. SIEM (eng. Security Information and Event Management) rješenja postaju glavni dio sigurnosne infrastrukture svake organizacije. SIEM tehnološki projekti su tipično orijentirani na nekoliko većih slučajeva korištenja: izvještavanje o regulatornoj sukladnosti (npr. PCI DSS[2], ISO27001[3], …), upravljanje prijetnjama, odgovaranje na incidente i forenziku.

Logovi sa svih mrežnih uređaja, servera, aplikacija za upravljanje identitetima i pristupa resursima, baza podataka te drugih servisa u sustavu prikupljaju se na jednom mjestu radi obrade i generiranja izvještaja, te arhiviranja. SIEM sustav prikupljene logove i događaje analizira, uzimajući u obzir njihovu korelaciju te automatski generira upozorenja i izvještaje u realnom vremenu. Ovisno o potrebi, može se podesiti i slanje notifikacija za potencijalno opasne događaje. Na jednoj konzoli prikazuju se upozorenja s cijele mreže, prezentiraju i povezuju informacije, generiraju izvještaji te radi dugoročna pohrana sigurnosnih informacija. Fokus je na praćenju i upravljanju korisničkim i servisnim pravima, imeničkim servisima, praćenju aktivnosti na mreži i promjena u sustavu, reviziji logova i upravljanju odgovorima na prijetnje. Arhivirane logove nije moguće mijenjati ili brisati u svrhu prikrivanja aktivnosti. Unaprijeđenije izvještavanja o regulatornoj suglasnosti i identificiranje sigurnosnih incidenata su glavni razlozi postavljanja ovog rješenja.

Spektar proizvoda koji pokrivaju dio ili cjelovito područje SIEM-a kreće od sustava za sakupljanje i arhiviranje sistemskih zapisa (logova) s osnovnim mogućnostima izvještavanja i uzbunjivanja, do SIEM sustava koji podržavaju prikupljanje, analizu i korelaciju log podataka u realnom vremenu, te naprednih mogućnosti automatiziranih akcija i forenzičkih upita, analiza, itd. Sva ta rješenja podržavaju dugotrajno čuvanje sistemskih zapisa i izvještavanje nad prikupljenim podacima, te se integriraju s postojećim mrežnim, sigurnosnim i infrastrukturnim aplikacijama i uređajima. Podržani su svi vodeći formati sistemskih zapisa (Windows Log, SysLog, SNMP, W3C, MS SQL Audit Log, Oracle Audit Log, IBM DB2 Audit Log, AS400 Audit Log, …). SIEM rješenja također mogu nadzirati i korelirati događaje na aplikacijskoj razini ili transakcijske logove u svrhu otkrivanja kombinacija događaja koje su indikator prevara ili neovlaštenog korištenja sustava.

Kritični događaji često ostaju neprimijećeni jer nema načina da se vidi uzročno-posljedična povezanost važnih događaja ili nema prikladnog procesa nadgledanja sustava. SIEM rješenje ne sprječava ili umanjuje napade samo po sebi, ali kada je instalirano kao dio veće sigurnosne infrastrukture onda može odigrati kritičnu ulogu u detekciji prijetnji, pravovremenoj reakciji i kasnijoj analizi. Mnogi uređaji, aplikacije i sam operacijski sustav generiraju logove koji se mogu iskoristiti za analizu i poboljšanje sigurnosti sustava. Međutim, ručna obrada i analiza nije učinkovita te je potrebno taj postupak automatizirati. U slučaju velikih organizacija, količina logova može biti iznimno velika. Problemom pohrane i pretraživanja logova bave se alati za upravljanje logovima, nakon čega se nekim alatom spremljeni logovi analiziraju.

Sustavi SIEM-a objedinjuju alate za upravljanje i alate zaspremanje logova, uz neke dodatne mogućnosti koje nude. Oni mogu obrađivati i velike količine logova dnevno, količinu koja je donedavno bila nezamisliva. Njihova se funkcionalnost i rad mogu podijeliti na dvije kategorije – upravljanje informacijama (prikupljanje, skladištenje, pretraživanje) te analiza, u kojoj se iz prikupljenih informacija raznim metodama nastoji automatski pronaći eventualne sigurnosne prijetnje. Korištenjem sustava SIEM tako je moguće poboljšati sigurnosnu politiku u organizaciji. Do sada je relativna složenost sustava SIEM u odnosu na obično pretraživanje logova često odbijala korisnike. U budućnosti težit će se ka što jednostavnijem korištenju.

Osim toga, potrebno je dodatno unaprijediti metode analize kako bi rezultati i korist od sustava SIEM bili što veći, a broj lažnih rezultata minimiziran. Uporaba SIEM alata, razvojem dodatnih pravila tijekom redovite uporabe i punjenjem baze znanja, omogućuje automatizaciju sustava praćenja i izvješćivanja baziranih na znanjima o prethodno uočenim i riješenim sigurnosnim incidentima te na taj način skraćuje vrijeme potrebno za otklanjanje sigurnosnog incidenta.

U idućim poglavljima ovog rada dati ćemo kratak prikaz potencijalnih napada i/ili prijetnja na informacijske sustave, SIEM sustav kroz njegove osnovne karakteristike, te ćemo objasniti rad istog sustava na primjeru *ArcSighta*, koje je jedno od vodećih rješenja.